DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

Monthly Report to Congress of Data Incidents
August 29 - October 2, 2011

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066182	Mishandled/ Misused Physical or Verbal Information	VISN 18 Tucson, AZ	8/29/2011	9/1/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	8/29/2011	INC000000168950	N/A	N/A	N/A	1	

Incident Summary

An electrocardiogram (EKG) printout was found still connected to an open EKG machine in a busy hallway on an inpatient ward. This affected one (1) patient.

Incident Update

08/29/11:
The document was left unattended for over 30 minutes and contained the patient's full name, SSN, date of birth, and medical information. The patient will be offered credit protection services.

NOTE: There were a total of 93 Mis-Handling incidents this reporting period. Because of repetition, the other 92 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The patient was notified and the Privacy Officer provided staff with additional training to ensure that this type of incident does not occur again.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066215	Mishandled/ Misused Physical or Verbal Information	VISN 23 Des Moines, IA	8/29/2011	9/6/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	8/29/2011	INC000000169027	N/A	N/A	N/A		1

Incident Summary

Veteran A received Veteran B's medication in the mail. The information disclosed includes Veteran B's name and type of medication.

Incident Update

08/30/11:
Veteran B will receive a letter of notification.

NOTE: There were a total of 90 Mis-Mailed incidents this reporting period. Because of repetition, the other 89 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

Pharmacy is working on a plan to decrease the number of mis-mailed prescriptions.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066265	Missing/Stolen Equipment	VISN 17 Temple, TX	8/30/2011	9/6/2011	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	8/30/2011	INC000000169280	N/A	N/A	N/A		

Incident Summary

A Dell desktop computer was reported missing/stolen from the Ear, Nose and Throat (ENT) Clinic. Office of Information and Technology (OIT) staff and VA Police were promptly informed. Per the OIT Assets Manager, desktop computers are not encrypted, but just like any other computer or laptop, the user's "My Documents" folder resides on a network drive, and is not stored locally on the hard drive.

Incident Update

08/31/11:
The desktop computer was used by a clinic clerk to access VistA and CPRS and conduct administrative activities. Patients are seen every day in the clinic. The desktop computer is located in an open clinic area. The clerk left work on Friday afternoon at the completion of her tour of duty and when she reported to work on Monday, the computer tower was gone. There is no personally identifiable information (PII) or protected health information (PHI) stored on the desktop computer.

Resolution

The VA Police completed their investigation and the information Security Officer (ISO) received a copy of the Uniform Offense Report (UOR). The UOR indicates that when the employee reported for duty, she noticed the desktop computer tower at her work station was missing. Per the VA Police UOR, the disposition states there are no suspects or witnesses at this time and it is unknown what happened to the missing computer tower.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066332	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Charleston, SC	9/1/2011	9/20/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	9/1/2011	INC000000169577	N/A	N/A	N/A		1

Incident Summary

Patient A received one non-controlled substance medication intended for Patient B. The medication item contained Patient B's name and medication name. No SSN data was compromised. Patient A contacted the Salisbury VAMC to report the error. The Salisbury VAMC returned the incorrect medication to CMOP Charleston. The investigation reveals that Patient B's medication item was inadvertently combined into a package with Patient A's shipping label as a result of human error. Appropriate employee retraining and counseling will be performed.

Incident Update

09/01/11:
Patient B will be sent a notification letter.

NOTE: There were a total of 8 Mis-Mailed CMOP incidents out of 7,657,443 total packages (11,190,955 total prescriptions) mailed out for this reporting period. Because of repetition, the other 7 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Resolution

The employee was counseled and retrained in proper packing procedures.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066430	Missing/Stolen Equipment	VACO OI&T Washington, DC	9/2/2011	9/6/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0515338	9/2/2011	INC000000169870	N/A	N/A	N/A		

Incident Summary

An iPad2 device was stolen from a VA office. The device was not configured to connect to the VA network for email or data. The data service was cancelled. The VA Police were contacted and provided a report. No VA sensitive data was stored on the device.

Incident Update

09/06/11:
The iPad2 was new and had never been issued to an employee. It had not been configured for employee use. The signal for the iPad2 was killed as soon as it was discovered as missing. The VA Police are reviewing security camera activity.

Resolution

The device was not found. A Security and Law Enforcement staff member is looking through the camera footage at the access and exit points on the third floor for any additional information.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066464	Missing/Stolen Equipment	VISN 10 Cincinnati, OH	9/6/2011		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	9/6/2011	INC000000170123	N/A	N/A	N/A		

Incident Summary

A VA nurse was preparing an exam room for a patient and noticed that the computer, monitor, keyboard, mouse, and cables that were usually located in that exam room were all missing. The computer was last seen in that room on Friday afternoon. A VA Police report has been initiated.

Incident Update

09/12/11:
The Information Security Officer (ISO) states that the desktop computer was not encrypted, however, staff are instructed to never save anything to the local hard drive. Staff members are instructed to use their network share drives, however, given the number of people that may have used this computer it is not currently possible to determine if all staff followed the policy. Police are investigating this loss and reviewing door check logs and surveillance tapes.

09/19/11:
Per the ISO, the investigation is continuing.

10/04/11:
Surveillance cameras do not cover the vantage points needed to monitor activity where this computer was located. The police case will be left as ongoing due to insufficient evidence or leads.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066484	Missing/Stolen Equipment	VISN 02 Buffalo, NY	9/6/2011	9/7/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	9/6/2011	INC000000170190	N/A	N/A	N/A		

Incident Summary

The Facility Chief Information Officer (FCIO) reported that a Dell Latitude C600 laptop was recently reimaged and placed in secured storage. The laptop was in storage as a backup (this model of laptop is no longer in use). There was no personally identifiable information (PII) or protected health information (PHI) stored on the laptop. The FCIO stated that this was an old laptop and was going to be used as a spare. The laptop may have been turned in for excess without the proper paperwork being completed.

Incident Update

09/06/11:
No data breach occurred. The laptop was reimaged, secured and had not been reissued.

09/15/11:
The FCIO confirmed that the laptop was not encrypted. It was an older model kept solely for Bar Code Medication Administration (BCMA) back-up purposes. It was also confirmed the laptop had definitely been cleared of all data, reimaged and had not been put back into service.

Resolution

The Information Security Officer (ISO) and FCIO discussed the security of the area and how to maintain better inventory control of IT equipment. They will educate the staff on the need to keep the area secured when no one is present.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066531	Mishandled/ Misused Physical or Verbal Information	VISN 04 Philadelphia, PA	9/7/2011	9/28/2011	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	9/7/2011	INC000000170383	N/A	N/A	N/A	130	

Incident Summary

During a training class, a sign-in roster was distributed with names and social security numbers.

Incident Update

09/07/11:
According to the Information Security Officer (ISO), the Environmental Management Service (EMS) Section Chief printed the roster as a sign-in sheet for a class of 148 employees. The Section Chief admitted that he inadvertently printed the roster with the SSN included. Therefore, 148 employees will be sent a letter offering credit protection services.

09/12/11:
The revised count is 130 individuals.

Resolution

The staff member was counseled for inappropriate use of SSN.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066620	Missing/Stolen Equipment	VISN 11 Detroit, MI	9/9/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	9/9/2011	INC000000170815	N/A	N/A	N/A		

Incident Summary

During an inventory the department was looking for items on their Equipment Inventory List (EIL). The EIL was due to be completed in May, and they have been looking for items since that time. It was determined that the computer had been missing on 08/26/11 when they completed the Report of Survey (ROS), however, the VA Police report just states 34 items are missing.

Incident Update

09/12/11:
It was reported by the Information Security Officer (ISO) that there is only one computer missing, out of the 34 items. The computer was usually located in the Surgical Suite and it is very unlikely that there was any data on the local hard drive as there are group polices in place to prevent users from saving data to the local hard drive. The investigation is continuing.

NOTE: There were a total of two IT Equipment Inventory Incidents this reporting period. Because of repetition, the other one is not included in this report, but is included in the "IT Equipment Inventory Incidents" count at the end of this report.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066925	Mishandled/ Misused Physical or Verbal Information	VISN 20 Walla Walla, WA	9/19/2011		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	9/19/2011	INC000000172229	N/A	N/A	N/A		212

Incident Summary

The Community Based Outpatient Clinic (CBOC) Nurse Manager was tidying the waiting room and found a printed list of patients that were enrolled in the home oxygen program. The Manager had gone through the waiting room at 7:00 AM and the documents were not found at that time. At 2:30 PM the documents were found on an end table in the waiting room with blank documents for My HealtheVet enrollment. The Care Coordination Home Telehealth (CCHT) nurse generated the list and passed it off to a Health Technician (HT). The HT gave the document back to the CCHT nurse. The CCHT nurse gave the document to a Medical Service Assistant (MSA). The Privacy Officer (PO) is still investigating what took place after this. The information on the list included the patients' names, partial SSNs, the provider's name, date and clinic in which the patient is being treated.

Incident Update

09/21/11:
The CBOC Nurse Manager is investigating. Apparently the CCHT nurse printed a list of 212 patients and asked either the HT and/or MSA to obtain the providers' names and then to contact the patients to recruit them for Home Telehealth services.

09/26/11:
The 212 patients will receive a letter of notification.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066980	Missing/Stolen Equipment	VISN 09 Memphis, TN	9/21/2011	9/28/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	9/21/2011	INC000000172548	N/A	N/A	N/A		

Incident Summary

Chemotherapy room D425 was entered after hours. This area was locked. A VA laptop computer was stolen along with personal items of one of the employees. The personal items were removed from the second employee's locker. A lock was removed from an employee's locker.

A VA nurse employee discovered the VA laptop missing on September 21, 2011 at approximately 7:30 AM, upon her arrival. The laptop was attached to a mobile cart with a cable lock. The cable lock was broken but other items on the mobile cart were still in place (hand held scanner, mouse, keyboard). The laptop is used for Bar Code Medication Administration (BCMA) on inpatients during normal business hours. At the end of the shift, 4:30 PM, two nurses which worked in the area were the last to see the laptop before locking the area doors. The Nurse Manager ensured all outer doors leading to hallway were locked so the area was secured. The VA Police checked with Environmental Management Service (EMS) and verified that no housekeeping staff were in the area last evening. There are no signs of forced entry, yet the doors were unlocked upon the employees' arrival to the work area. The lock on laptop cable was broken.

The Information Security Officer (ISO) contacted OI&T for information on the VA laptop. The laptop is not encrypted, but the hard drive is locked so users are unable to save data.

Incident Update

09/21/11:
This incident involves the theft of government equipment and personal items. The laptop is not encrypted, but the hard drive was locked so users are unable to save data. There was no data stored on the VA laptop. No data breach occurred.

Resolution

Office of Information and Technology staff are in the process of encrypting all BCMA laptops.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067351	Missing/Stolen Equipment	VISN 21 Martinez, CA	9/30/2011	10/4/2011	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	9/30/2011	INC000000174356	N/A	N/A	N/A		

Incident Summary

A scientific research contractor reported that an experimental research program was being conducted where a patient is chosen and given a special computer that is set up in his residence for the purpose of interacting with hearing impaired VA patients. The computer was brand new. The computer contained no patient information that could be in violation of HIPPA. The computer was reported missing or stolen just one day after it was delivered on 08/31/2011. The PC was ordered and used for a research protocol. The PC did not have any sensitive data on it. It was never connected to the network. A waiver, # 201, was submitted and approved to have the patients use the PCs in their homes.

Resolution

No data breach occurred.

Total number of Lost Blackberry Incidents	24
Total number of Internal Un-encrypted E-mail Incidents	86
Total number of Mis-Handling Incidents	93
Total number of Mis-Mailed Incidents	90
Total number of Mis-Mailed CMOP Incidents	8
Total number of IT Equipment Inventory Incidents	2
Total number of Missing/Stolen PC Incidents	4
Total number of Missing/Stolen Laptop Incidents	17 (15 encrypted)